Jednotné přihlašování

Technologie jednotného přihlašování (anglicky single sign-on, nebo také SSO) fungují na principu univerzálního klíče. Uživatel má své přihlašovací údaje uložené na jednom centrálním místě a používá je k přihlášení u různých internetových služeb. Tyto internetové služby pak nemají k jeho přihlašovacím údajům vůbec přístup. Celý mechanismus bývá často rozšířen o možnost jednotné správy osobních údajů. Aby nebylo nutné při registraci k nové internetové službě znovu zadávat své osobní údaje jako jméno, e-mail, doručovací adresu nebo fakturační adresu, nabízí tyto technologie možnost rovnou z jednoho centrálního místa tyto údaje službě předat. Toto je samozřejmě možné pouze po jednoznačné identifikaci uživatele a s jeho souhlasem. Popsaný mechanismus předávání údajů je možné využívat opakovaně a využít jej k aktualizaci údajů. Stačí, když si opravíte údaj na centrálním místě a jednotlivé služby, ke kterým se přihlašujete si mohou tento údaj automaticky aktualizovat.

Výhody jednotného přihlašování

Hlavní výhodou je vyšší komfort při využívání Internetu, neboť odpadá opakované zadávání stejných údajů. Statistiky také ukazují, že uživatelé opakovaně používají stejná hesla u více různých služeb, což zvyšuje riziko, že heslo unikne do nepovolaných rukou a bude zneužito. Uložení silného hesla na jednom místě toto riziko prozrazení minimalizuje. Navíc služby poskytující možnost jednotného přihlášení často nabízejí silnější metody přihlašování jako například přihlášení osobním certifikátem. S použitím certifikátu má uživatel všechny citlivé údaje přímo u sebe na svém počítači nebo čipové kartě a ani poskytovatel služby jednotného přihlášení k nim nemá přístup.

V některých případech tito centrální správci elektronických identit přidávají ověřování údajů. Mnoho internetových služeb totiž vyžaduje, aby uživatel byl skutečná fyzická osoba a tyto služby pak vynakládají nemalé částky na ověření této skutečnosti. Pokud již k tomuto ověření ale jednou dojde, u ostatních služeb se jedná o duplicitní proces, který přináší zbytečné výdaje a navíc obtěžuje uživatele, který si celým procesem musí projít znovu. Technologie jednotného přihlašování spolu s centrální správou osobních údajů v tomto směru nabízejí elegantní řešení. K ověření dojde na jednom místě a služby, které požadují ověření údajů, si tento stav ověření mohou samy zkontrolovat.

Rizika jednotného přihlašování

Největší riziko souvisí principiálně s používáním univerzálních klíčů. V případě, že dojde ke zcizení takového klíče, jeho držitel získá přístup k mnohem většímu počtu dveří, než v případě jednoúčelového klíče. Každopádně i v případě reálných klíčů stejně lidé, přestože nemají jeden klíč na všechno, nosí běžně všechny své klíče na jedné klíčence a z pohledu rizika ztráty je to tedy stejné jako kdyby měli jeden univerzální klíč. Nesporné výhody, které univerzální klíče a jednotné přihlašování přinášejí, tedy musí být adekvátně vyváženy zvýšenou ochranou takových univerzálních přístupů. Prakticky to znamená vybírat si za tímto účelem důvěryhodné správcovské firmy a pokud možno používat bezpečnější metody přihlášení než jenom obyčejné heslo.

Dalším důležitým faktem, se kterým je nutné počítat, je skutečnost, že správcovská firma má

přirozeně informace o všech vašich přihlášeních k internetovým službám. Přes tuto firmu totiž musí projít každé vaše přihlášení. Znamená to opět zvážit, zda vámi zvolená společnost pro centrální správu údajů a jednotné přihlašování je dostatečně důvěryhodná a vaše digitální stopa, která u ní vzniká, nebude zneužita. Je to ale v zásadě stejný typ důvěry, který vkládáte do svého poskytovatele připojení k Internetu, neboť i tato firma ví přesně, na které adresy jejím prostřednictvím přistupujete.

Kde si jednotné přihlašování pořídit

Asi nejrozšířenějšími službami, které nabízejí možnost uchovávat jednotné přihlašovací údaje, jsou Facebook, Google nebo u nás Seznam. Tyto komerční společnosti tuto možnost nabízejí spíš jako bonus k jejich dalším službám a například nijak negarantují validitu údajů jimi spravovaných účtů. V české akademické sféře existuje projekt EduID, za kterým stojí sdružení CESNET, který se snaží podobným způsobem propojit akademické instituce. Pokud máte například účet u některé školy zapojené do tohoto projektu, můžete své přihlašovací údaje používat u množství další zejména akademických internetových služeb.

Nejnovějším příspěvkem v této oblasti je služba mojeID, za kterou stojí sdružení CZ.NIC, správce české narodní domény .CZ. Tato služba umožňuje několikastupňové ověřování uživatelových dat a také bezpečnější metody přihlášení.

Kde jednotné přihlašování používat

Výhody jednotného přihlašování uživatel ocení až v momentu, kdy je může používat u velkého množství služeb, na které běžně přistupuje. Například pro službu mojeID je to možné již na desítkách českých služeb. Poznají se podle toho, že je na přihlašovací stránce uvedeno buď logo služby mojeID nebo logo OpenID, což je název technologie použité pro implementaci služby mojeID.